AF/2143

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/823,616
Filing Date	March 31, 2001
First Named Inventor	Simon Knee
Art Unit	2143
Examiner Name	Bilgrami, A.
Total Number of Pages in This Submission	24
Attorney Docket Number	42390P9020

ENCLOSURES ***(check all that apply)***

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Return postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Gordon R. Lindeen III, Reg. No. 33,192 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	January 29, 2007

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Debbie Casias**		
Signature	Debbie Casias	Date	**January 29, 2007**

Based on PTO/SB/21 (09-04) as modified by Blakely, Sokoloff, Taylor & Zafman (ndc) 10/12/2006.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Our Docket No.: 42390P9020

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Knee et al.	)	Examiner: Bilgrami, A
	)	
Application No.: 09/823,616	)	Art Group: 2413
	)	
Filed: March 31, 2001	)	
	)	
For: First Classless Inter-Domain Routing (CIDR) Lookups	)	

Mail Stop: Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SECOND SUBSTITUTE APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

This Appeal Brief is a second substitute for the Appeal Brief previously filed on November 21, 2005. This version explicitly provides a mapping of each of the independent claims instead of referring to other claims by reference.

Applicant (hereinafter "Appellant") hereby submits this Appeal Brief (hereinafter "Brief") in support of its appeal from a final decision by the Examiner, mailed June 17, 2005, in the above-referenced Application. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals and Interferences (hereinafter "Board") for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1-32 are currently pending in the above-referenced application. No claims have been allowed. Claims 1-32 were rejected in the Final Office Action mailed June 17, 2005, and are the subject of this appeal.

Claims 1-32 stand rejected under 35 U.S.C. § 102. .

IV. STATUS OF AMENDMENTS

In response to the Final Office Action mailed on June 17, 2005, rejecting claims 1-32, Appellant timely filed a Notice of Appeal on September 16, 2005.

A copy of all claims on appeal is attached hereto as Appendix A

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Introduction

"The networking community has adopted the Classless Inter-Domain Routing (CIDR) scheme in which addresses are allocated in contiguous blocks of any size that can be described as two taken to an integer power. Routers, which forward packets from one device to another, can save space in their routing tables by maintaining forwarding instructions for the address blocks rather than individual addresses. However, some difficulty arises in that, depending on the router's position within the network, it might have to treat some addresses within a block differently than the others." See Background of the Invention, page 2, lines 9-15

"Specifically, if an IP destination address matches more than one entry in the routing table, the router should forward the packet according to the forwarding instructions associated with the entry having the most "specific" matching routing table entry, e.g., the "longest match" or the "best prefix match." An IP address comprises a portion identifying a network prefix and a portion identifying a host number. An IP address with a longer network prefix describes a smaller set of destinations and is said to be more specific than an IP address with a shorter network prefix. Therefore, when forwarding traffic, a network device must choose the entry with the longest matching network prefix. The length of an entry's network prefix may be identified by a length attribute or by a "mask" associated with the entry." See Background of the Invention, page 2, line 20 to page 3, line 3.

Claim 1

Referring to Claim 1, it is directed to a new "method of performing a longest match search" which begins with "receiving (510, 520, 710) a search key, including an

address." As stated at paragraph 0036, "the search key typically comprises the source or destination IP address embedded in the packet's header."

The next element recites, "retrieving (720) an encoded mask vector (670) from a mask table (240, 650), the encoded mask vector corresponding to an address of the search key." The correspondence is described in paragraph 0047 with reference to Figure 6.

The next element recites "determining (520, 740, 770) a set of masks using the encoded mask vector (mask vector expansion at para. 0056) that when applied to the search key are known to have a potential for matching an entry in a routing table (230, 300, 600)." As stated at paragraph 0040, rather than simple-mindedly using a mask reduced by one bit for the generation of each successive routing table query..., based upon knowledge of the routing table 230, the set of masks generated in block 520 excludes those masks that would result in a fruitless routing table search." Determining the masks according to the ripple technique is described at paragraph 0052.

The next element recites, "forming (530, 750, 760) a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector (670) to be the longest mask of the set of masks."

The last element recites, "applying (540) the routing table query to the routing table (600)." "Briefly, the longest match search process queries the routing table 230 once per iteration looking for an entry that matches a search key (para. 0049)."

Claim 8

Claim 8 is directed to a packet forwarding device with the following elements:

a plurality of ports 210 upon which packets are received and transmitted (para. 0025), the packets including an address (para. 0036);

a routing processor 220 coupled to the plurality of ports to determine an egress port 210 of the plurality of ports for a packet received on an ingress port 210 of the

plurality of ports (para. 0025) by performing a longest match search (para. 0049) comprising one or more routing table queries, the routing table queries being based on the packet address and a mask indicated by an encoded mask vector of a mask table to be the longest mask of a set of masks determined using the encoded mask vector;

a routing table 230, coupled to the routing processor, to provide the routing processor with a match indication and information regarding a matching routing table entry, if any, of a plurality of routing table entries stored therein in response to a routing table query (para. 0042); and

a mask table 240, coupled to the routing processor, to maintain encoded mask vectors corresponding to packet addresses, the encoded mask vectors identifying mask lengths of the plurality of routing table entries (para.0028).

Claim 12

Claim 12 is directed to a method of forwarding a packet with the following elements.

receiving 410 a packet on an ingress port 210 of a plurality of ports (para. 0036);

extracting 420 a destination Internet Protocol (IP) address from a header of the packet (paras. 0027, 0036);

using a portion of the destination IP address to index into a mask table 240 to retrieve 520 an encoded mask vector that identifies a series of masks to be applied to the destination IP address during a longest match search 430 of a routing table, the series of masks representing those masks that are known to have a potential for matching an entry in the routing table when applied to the destination IP address (paras. 0029, 0036 0040);

identifying 440, 550 a longest matching entry in the routing table by performing the longest match search based upon the destination IP address and one or more of the series of masks (para. 0042); and

forwarding 460 the packet to a network device associated with the destination IP address via an egress port of the plurality of ports identified by the longest matching entry (para. 0036).

Claim 16

Claim 16 is directed to a machine-readable medium to cause the processor to perform the operations of Claim 1. The machine-readable medium is described on page 9, lines 1-17. The medium may be embodied in the routing process 220, see page 10, lines 7-16. The claim begins with "receive (510, 520, 710) a search key, including an address." As stated at paragraph 0036, "the search key typically comprises the source or destination IP address embedded in the packet's header."

The next element recites, "retrieve (720) an encoded mask vector (670) from a mask table (240, 650), the encoded mask vector corresponding to an address of the search key." The correspondence is described in paragraph 0047 with reference to Figure 6.

The next element recites "determine (520, 740, 770) a set of masks using the encoded mask vector (mask vector expansion at para. 0056) that when applied to the search key are known to have a potential for matching an entry in a routing table (230, 300, 600)." As stated at paragraph 0040, rather than simple-mindedly using a mask reduced by one bit for the generation of each successive routing table query..., based upon knowledge of the routing table 230, the set of masks generated in block 520 excludes those masks that would result in a fruitless routing table search." Determining the masks according to the ripple technique is described at paragraph 0052.

The next element recites, "form (530, 750, 760) a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector (670) to be the longest mask of the set of masks."

The last element recites, "apply (540) the routing table query to the routing table (600)." "Briefly, the longest match search process queries the routing table 230 once per iteration looking for an entry that matches a search key (para. 0049)."

Claim 19

Claim 19 is directed to the operations of Claim 12 recited in a step-plus-function format. Claim 19 is directed to a forwarding a packet with the following steps.

a step for receiving 410 a packet on an ingress port 210 of a plurality of ports (para. 0036);

a step for extracting 420 a destination Internet Protocol (IP) address from a header of the packet (paras. 0027, 0036);

a step for using a portion of the destination IP address to index into a mask table 240 to retrieve 520 an encoded mask vector that identifies a series of masks to be applied to the destination IP address during a longest match search 430 of a routing table, the series of masks representing those masks that are known to have a potential for matching an entry in the routing table when applied to the destination IP address (paras. 0029, 0036 0040);

a step for identifying 440, 550 a longest matching entry in the routing table by performing the longest match search based upon the destination IP address and one or more of the series of masks (para. 0042); and

a step for forwarding 460 the packet to a network device associated with the destination IP address via an egress port of the plurality of ports identified by the longest matching entry (para. 0036).

Claim 23

Claim 23 is directed to the operations of Claim 1 recited in a step-plus-function format. The claim is directed to "performing a longest match search" which begins with

"a step for receiving (510, 520, 710) a search key, including an address." As stated at paragraph 0036, "the search key typically comprises the source or destination IP address embedded in the packet's header."

The next element recites, "retrieving (720) an encoded mask vector (670) from a mask table (240, 650), the encoded mask vector corresponding to an address of the search key." The correspondence is described in paragraph 0047 with reference to Figure 6.

The next element recites "a determining step for determining (520, 740, 770) a set of masks using the encoded mask vector (mask vector expansion at para. 0056) that when applied to the search key are known to have a potential for matching an entry in a routing table (230, 300, 600)." As stated at paragraph 0040, rather than simple-mindedly using a mask reduced by one bit for the generation of each successive routing table query..., based upon knowledge of the routing table 230, the set of masks generated in block 520 excludes those masks that would result in a fruitless routing table search." Determining the masks according to the ripple technique is described at paragraph 0052.

The next element recites, "a step for forming (530, 750, 760) a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector (670) to be the longest mask of the set of masks."

The last element recites, "a step for applying (540) the routing table query to the routing table (600)." "Briefly, the longest match search process queries the routing table 230 once per iteration looking for an entry that matches a search key (para. 0049)."

Claim 29

Claim 29 is directed to the limitations of Claim 8 recited in a means-plus-function format. For Claim 29, the structures in the specification are described as mentioned in Claim 8. Claim 29 is directed to a packet forwarding device with the following elements:

a plurality of interface means 210 for receiving and transmitting packets (para. 0025), the packets including an address (para. 0036);

routing processor means 220 coupled to the plurality of interface means, for determining an egress interface 210 of the plurality of interface means by performing a longest match search (para. 0049) comprising one or more routing table queries, the routing table queries being based on the packet address and a mask indicated by an encoded mask vector of a mask table to be the longest mask of a set of masks determined using the encoded mask vector;

a routing table means 230, coupled to the routing processor means, for providing the routing processor means with a match indication and information regarding a matching routing table entry, if any, of a plurality of routing table entries stored therein in response to a routing table query (para. 0042); and

a mask table means 240, coupled to the routing processor means, for maintaining encoded mask vectors corresponding to packet addresses, the encoded mask vectors identifying mask lengths of the plurality of routing table entries (para.0028).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-32 stand rejected under 35 U.S.C. §102(e) as being anticipated by Hunter et al., U.S. Publication No. 2002/0059197 A1 ("Hunter"). A reversal of this rejection is sought by this appeal.

There are no other rejections.

VII. ARGUMENT

CLAIM 1 CANNOT BE ANTICIPATED BY HUNTER WHERE HUNTER FAILS TO SHOW AN ENCODED MASK VECTOR, A SET OF MASKS, AND FORMING A QUERY BASED UPON A MASK.

The Examiner has rejected claims 1-32 under 35 U.S.C. §102 (e) as being anticipated by Hunter, U.S. Publication No. 2002/0059197 A2 ("Hunter"). Claim 1 refers to "retrieving an encoded mask vector from a mask table, the encoded mask vector corresponding to an address of the search key," to "determining a set of masks using the encoded mask vector," and to "forming a routing table query based upon the search key and a longest mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks."

The Examiner refers to paragraph 73 of Hunter as relating to the recitations referring to "retrieving an encoded mask." However, paragraph 73 describes only representing an address and its associated mask by embedding a mask length indicator in the address information of a forwarding database. There is no suggestion in Hunter of using a mask table that contains encoded mask vectors, nor of using an encoded mask vector when applying a search key to a routing table.

The Examiner also refers to paragraphs 41 and 42 which mention a longest match search. However, this section makes no mention of a separate mask table containing encoded mask vectors nor of using such a table in performing the longest match search.

Considering Hunter in more detail, Hunter, as shown in Figure 6 produces a 16-bit hash index." (step 610, para. 61, line 4), based on a current mask and the masked search key (para. 65, lines 2-5). The hash bin index is applied to search a hash bin (step 630) to find the most appropriate forwarding database entry. This would appear to

correspond to a forwarding address that would come out of a routing table as recited in Claim 1.

Two tests are applied to the result at step 640 based on the hash bin entry's mask length and its address information. If the result is not declared to be a match, then the hash index is modified (steps 650, 660, 620) and the search is tried again. If it is a match, then the process ends. Page 6 appears to discuss issues related to the iterative matching process of Figure 6.

Referring to Claim 1, after receiving a search key, it recites, "retrieving an encoded mask vector from a mask table." Hunter does not retrieve an encoded mask vector but creates a hash index using the current mask. Hunter does not appear to explain where this current mask comes from, but there is clearly no suggestion that it be obtained from an encoded mask vector.

Claim 1, then recites, "determining a set of masks using the encoded mask vector that when applied to the search key are known to have a potential for matching an entry in a routing table." Hunter does not determine a set of masks and does not use an encoded mask vector. Hunter generates a hash index using one mask. If there is no match, then step 660 shortens that same mask and generates another hash index (step 620) and so on until a mask is found.

Claim 1, further recites "forming a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks and applying the routing table query to the routing table." In Hunter, the routing table query would appear to correspond to applying the hash index to the hash bin (630).

Accordingly, Appellant finds nothing similar to the elements in Claim 1 that relate to the encoded mask vector, to determining a set of masks from the encoded mask

vector and to a set that is known to a have a potential for matching an entry in the routing table. Appellant has accordingly suggested that the claims are allowable over Hunter.

The Examiner suggests that Hunter discloses decimating a mask. Claim 1 does not recite decimating a mask but "determining a set of masks using the encoded mask vector."

The Examiner further suggests that Hunter discloses identifying a longest matching prefix of a given address in a forwarding database/routing table, referring to page 1 paragraph 4, inter alia. However, Claim 1 provides a different description for working with a routing table. "[F]orming a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks; and applying the routing table query to the routing table."

The Examiner further suggests that Hunter discloses that a hash index is generated based upon a mask and a masked search key and that this relates to an "encoded mask table." The mask table of Claim 1, however, provides an encoded mask vector from which a set of masks is determined. Hunter, as mentioned above, uses a current mask and applies it to a search. If there is no match, then the current mask is shortened. There is no set of masks and Hunter's current mask is not apparently generated from an encoded mask vector.

In the Advisory Action mailed September 12, 2005, the Examiner writes further that Hunter shows that "the hash index is used to search for an entry matching the masked search (page 5, paragraph 61, lines 1-16)." The claims of the present application do not refer to a hash index nor any use of a hash index.

VIII. CONCLUSION

Appellant respectfully submits that all the appealed claims in this application are patentable and requests that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

Please charge any shortages and credit any overpayment to out Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: January 29, 2007

Gordon R. Lindeen III
Reg. No. 33,192

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA. 90025-1030
(303) 740-1980

IX. APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

1. A method of performing a longest match search comprising:

receiving a search key, including an address;

retrieving an encoded mask vector from a mask table, the encoded mask vector corresponding to an address of the search key;

determining a set of masks using the encoded mask vector that when applied to the search key are known to have a potential for matching an entry in a routing table;

forming a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks; and

applying the routing table query to the routing table.

2. The method of claim 1, further comprising:

removing the longest mask from the set of masks; and

continuing to apply additional routing table queries until either the set of masks is empty or a matching entry is found in the routing table.

3. The method of claim 1, wherein the search key address comprises an Internet Protocol (IP) address.

4. The method of claim 3, wherein the IP address comprises a destination address.

5. The method of claim 3, wherein the IP address comprises a source address.

6. The method of claim 1, wherein the encoded mask vector has N bits and is capable of identifying N different length masks.

7. The method of claim 1, wherein the longest mask of the set of masks is determined by the following equation: Mask = (0 – MaskWord) | MaskWord,

where:

MaskWord is an encoded mask vector, and

Mask is the longest mask identified by MaskWord.

8. A packet forwarding device comprising:

a plurality of ports upon which packets are received and transmitted, the packets including an address;

a routing processor coupled to the plurality of ports to determine an egress port of the plurality of ports for a packet received on an ingress port of the plurality of ports by performing a longest match search comprising one or more routing table queries, the routing table queries being based on the packet address and a mask indicated by an encoded mask vector of a mask table to be the longest mask of a set of masks determined using the encoded mask vector;

a routing table, coupled to the routing processor, to provide the routing processor with a match indication and information regarding a matching routing table entry, if any, of a plurality of routing table entries stored therein in response to a routing table query; and

a mask table, coupled to the routing processor, to maintain encoded mask vectors corresponding to packet addresses, the encoded mask vectors identifying mask lengths of the plurality of routing table entries.

9. The packet forwarding device of claim 8, wherein the encoded mask vectors comprise N-bits and are capable of representing N different masks.

10. The packet forwarding device of claim 8, wherein the routing table comprises a Content Addressable Memory (CAM).

11. The packet forwarding device of claim 8, wherein the one or more routing table queries are formed by applying a series of masks determined with reference to the mask table to a search key extracted from the received packet.

12. A method of forwarding a packet comprising:

receiving a packet on an ingress port of a plurality of ports;

extracting a destination Internet Protocol (IP) address from a header of the packet;

using a portion of the destination IP address to index into a mask table to retrieve an encoded mask vector that identifies a series of masks to be applied to the destination IP address during a longest match search of a routing table, the series of masks representing those masks that are known to have a potential for matching an entry in the routing table when applied to the destination IP address;

identifying a longest matching entry in the routing table by performing the longest match search based upon the destination IP address and one or more of the series of masks; and

forwarding the packet to a network device associated with the destination IP address via an egress port of the plurality of ports identified by the longest matching entry.

13. The method of claim 12, wherein the portion of the destination IP address comprises the most significant N bits of the destination IP address.

14. The method of claim 12, wherein the encoded mask vector includes a plurality of mask length indicator bits that each indicate a mask length by virtue of their position within the encoded mask vector.

15. The method of claim 12, further comprising updating the mask table to include a new encoded mask vector in response to receiving a new routing table entry.

16. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to:

receive a search key, including an address;

retrieve an encoded mask vector from a mask table, the encoded mask vector corresponding to an address of the search key;

determine a set of masks using an encoded mask vector that when applied to the search key are known to have a potential for matching an entry in a routing table;

form a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks; and

apply the routing table query to the routing table.

17. The machine-readable medium of claim 16, wherein the longest mask of the set of masks is determined by the following equation: Mask = (0 – MaskWord) | MaskWord,

where:

MaskWord is an encoded mask vector, and

Mask is the longest mask identified by MaskWord.

18. The machine-readable medium of claim 16, wherein the encoded mask vector has N bits and is capable of identifying N different length masks.

19. A method of forwarding a packet comprising the steps of:

a step for receiving a packet on an ingress port of a plurality of ports;

a step for extracting an Internet Protocol (IP) address from a header of the packet;

a step for using a portion of the IP address to index into a mask table to retrieve an encoded mask vector that identifies a series of masks to be applied to the IP address during a longest match search of a routing table, the series of masks representing those masks that are known to have a potential for matching an entry in the routing table when applied to the IP address;

a step for identifying a longest matching entry in the routing table by performing the longest match search based upon the IP address and one or more of the series of masks; and

a step for forwarding the packet to a network device based upon the longest matching entry.

20. The method of claim 19, wherein the IP address comprises a destination IP address.

21. The method of claim 19, wherein the IP address comprises a source IP address.

22. The method of claim 19, wherein the encoded mask vector includes a plurality of mask length indicator bits that each indicate a mask length by virtue of their position within the encoded mask vector.

23. A method of performing a longest match search comprising the steps of:

a step for receiving a search key, including an address;

retrieving an encoded mask vector from a mask table, the encoded mask vector corresponding to an address of the search key;

a determination step for determining a set of masks using the encoded mask vector that when applied to the search key are known to have a potential for matching an entry in a routing table;

a step for forming a routing table query based upon the search key and a mask of the set of masks, indicated by the encoded mask vector to be the longest mask of the set of masks; and

a step for applying the routing table query to the routing table.

24. The method of claim 23, further comprising the steps of:

a step for removing the longest mask from the set of masks; and

a step for continuing to apply additional routing table queries until either the set of masks is empty or a matching entry is found in the routing table.

25. The method of claim 23, wherein the search key address comprises an Internet Protocol (IP) address.

26. The method of claim 23, wherein the encoded mask vector has N bits and is capable of identifying N different length masks.

27. The method of claim 23, wherein the longest mask of the set of masks is determined by the following equation: Mask = (0 – MaskWord) | MaskWord,

where:

MaskWord comprises an encoded mask vector, and

Mask comprises the longest mask identified by MaskWord.

28. The method of claim 27, further comprising:

isolating an endbit of the longest mask;

combining the longest mask with the inversion of the longest mask left-shifted one position; and

forming a subsequent routing table query based on the masked search key left-shifted one position and the endbit.

29. A packet forwarding device comprising:

a plurality of interface means for receiving and transmitting packets, the packets including an address;

routing processor means, coupled to the plurality of interface means, for determining an egress interface of the plurality of interface means for a packet received on an ingress interface of the plurality of interface means by performing a longest match search comprising one or more routing table queries, the routing table queries being based on the packet address and a mask indicated by an encoded mask vector of a mask table to be the longest mask of a set of masks determined using the encoded mask vector;

a routing table means, coupled to the routing processor means, for providing the routing processor means with a match indication and information regarding a matching routing table entry, if any, of a plurality of routing table entries stored therein in response to a routing table query; and

a mask table means, coupled to the routing processor means, for maintaining encoded mask vectors corresponding to packet addresses, the encoded mask vectors identifying mask lengths of the plurality of routing table entries.

30. The packet forwarding device of claim 29, wherein the encoded mask vectors comprise N-bits and are capable of representing N different masks.

31. The packet forwarding device of claim 30, wherein the routing table means comprises a Content Addressable Memory (CAM).

32. The packet forwarding device of claim 30, wherein the one or more routing table queries are formed by applying a series of masks determined with reference to the mask table means to a search key extracted from the received packet.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.